`https://example.com/` with an ACME client.

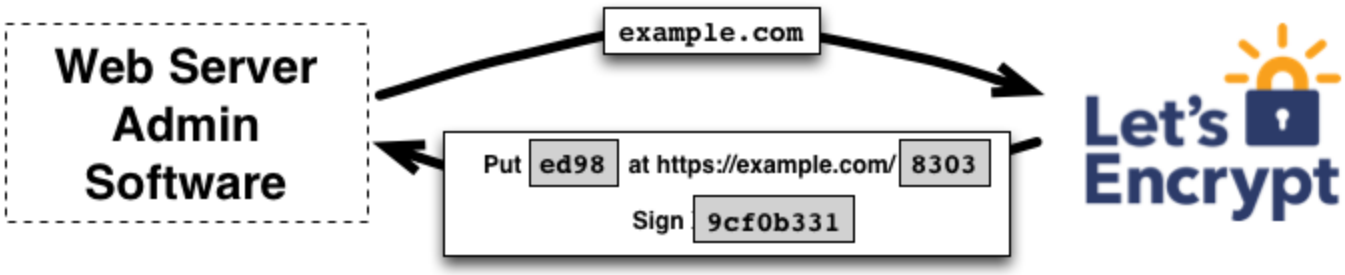
There are two steps to this process. First, the ACME client proves to the Certificate Authority (CA) that the web server controls a domain. After that the client can request or revoke certificates for that domain.

Domain Validation

Let's Encrypt identifies the ACME client software by public key. The first time the ACME client interacts with Let's Encrypt, it generates a new account key pair and proves to the Let's Encrypt CA that the operator controls one or more domains. This is similar to the traditional CA process of creating an account and adding domains to that account.

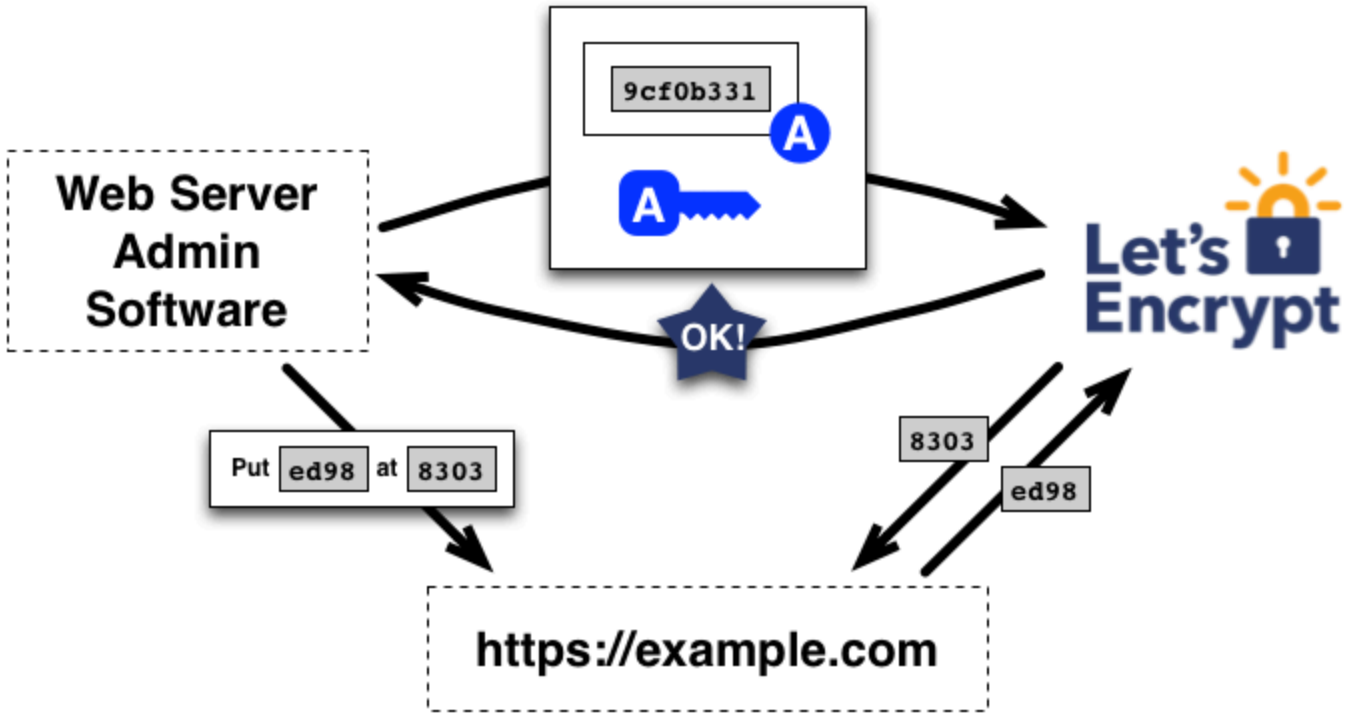
To kick off the process, the client asks the Let's Encrypt CA what it needs to do in order to prove that it controls `example.com`. The Let's Encrypt CA will look at the domain name being requested and issue one or more sets of challenges. There are different ways that the client can prove control of the domain. For example, the CA might give the client a choice of either:

- Provisioning a DNS record under `example.com`, or
- Provisioning an HTTP resource under a well-known URI on `http://example.com/`



The client software completes one of the provided sets of challenges. Let's say it is able to accomplish the second task above: it creates a file on a specified path on the `http://example.com` site. Once the client has completed these steps, it notifies the CA that it's ready to complete validation.

Then, it's the CA's job to check that the challenges have been satisfied from multiple network perspectives.



If the challenges check out, then the client identified by the public key is authorized to do certificate management for `example.com`.

Note that this process cannot use HTTPS, which makes it vulnerable to certain attacks. In order to mitigate the issue, Let's Encrypt actually performs multiple validations in parallel from different network perspectives. This makes it significantly harder for an attacker to successfully subvert the validation process.

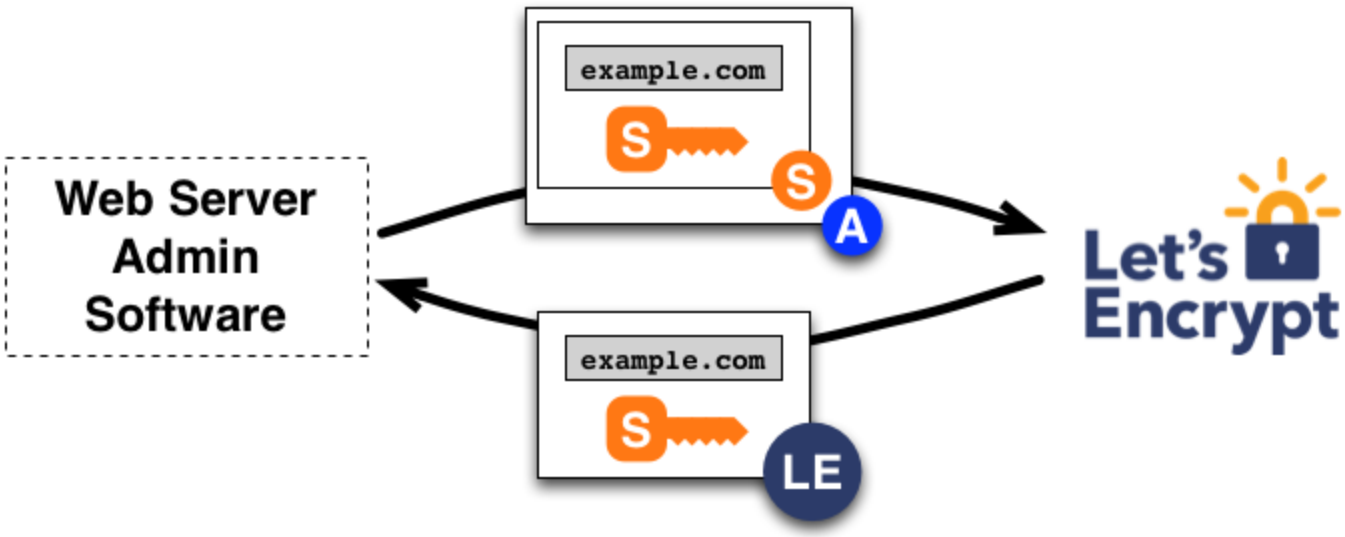
Certificate Issuance and Revocation

Once the client is authorized, requesting, renewing, and revoking certificates is simple—just send certificate management messages and sign them with the authorized account key pair.

Issuance

To obtain a certificate for the domain, the client constructs a PKCS#10 Certificate Signing Request (CSR) that asks the Let's Encrypt CA to issue a certificate for `example.com` with a specified public key. As usual, the CSR includes a signature by the private key corresponding to the public key in the CSR. The client also signs the whole CSR with the authorized key for `example.com` so that the Let's Encrypt CA knows it's authorized.

When the Let's Encrypt CA receives the request, it verifies both signatures. If everything looks good, it issues a certificate for `example.com` with the public key from the CSR and returns it to the client. The CA will also submit the certificate to numerous public Certificate Transparency (CT) logs. See here for more details.

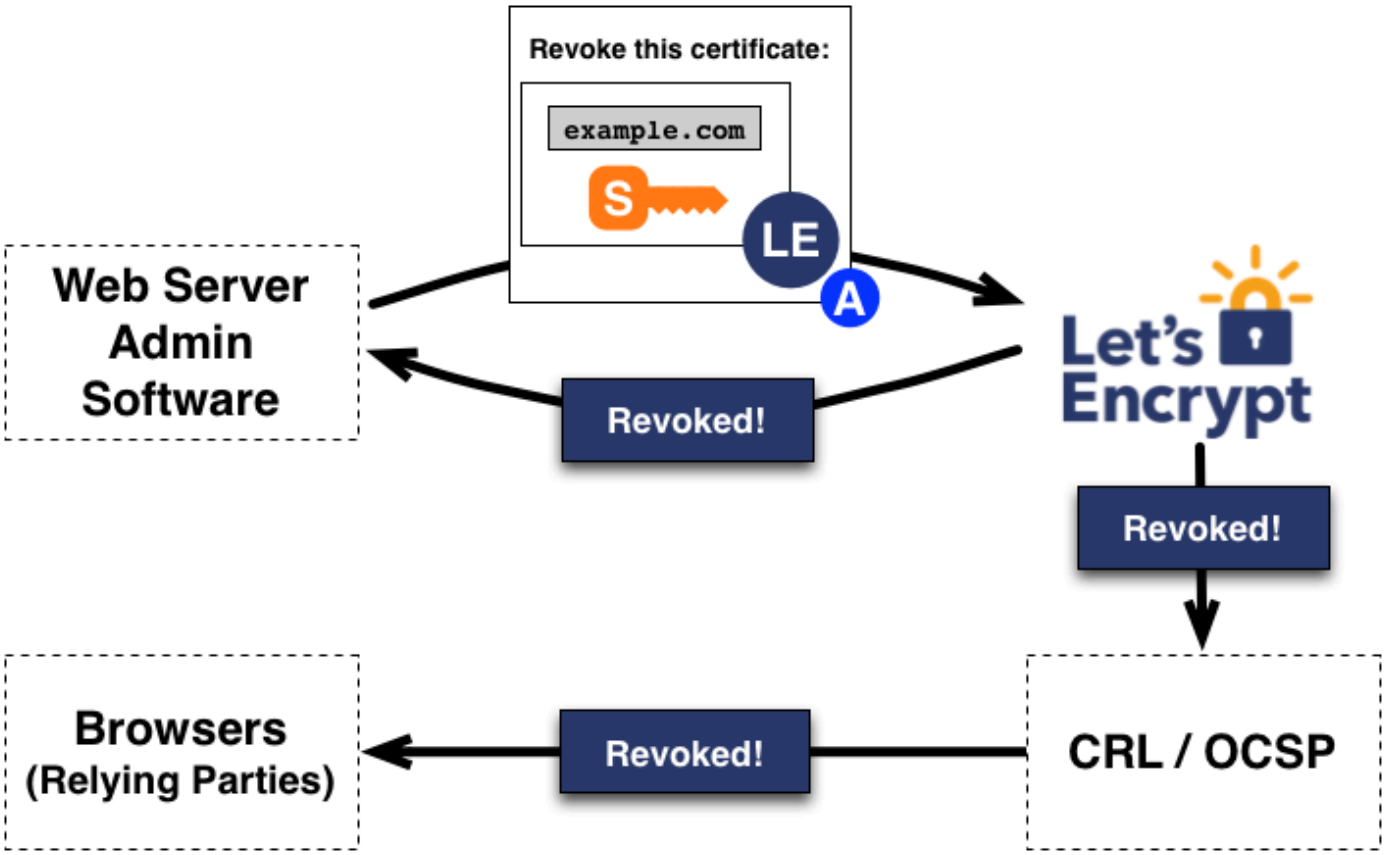


Renewing a certificate at a later time means repeating the issuance process over again - performing domain validation and then requesting a new certificate.

Revocation

Revocation works in a similar manner. The client signs a revocation request with the account key pair authorized for `example.com`, and the Let's Encrypt CA verifies that the request is authorized. If so, it publishes revocation information via Certificate Revocation List (CRL), so

that relying parties such as browsers can know that they shouldn't accept the revoked certificate.



ISRG

Let's Encrypt is a free, automated, and open Certificate Authority brought to you by the nonprofit Internet Security Research Group (ISRG). Read all about our nonprofit work this year in our 2025 Annual Report.

LEGAL ADDRESS
548 Market St, PMB 77519
San Francisco, CA 94104-5401
USA

SEND ALL MAIL OR INQUIRIES TO:
PO Box 18666
Minneapolis, MN 55418-0666
USA

SUBSCRIBE FOR EMAIL UPDATES ABOUT LET'S ENCRYPT AND OTHER ISRG PROJECTS

Email

- [ ] Brighter Bytes: the ISRG Newsletter
- [ ] Let’s Encrypt Technical Updates
- [ ] Let’s Encrypt Service Statistics
- [ ] Prossimo: Updates about our memory safety project
- [ ] Divvi Up: Updates about our privacy-respecting metrics project

Sign Up

Note: You can opt-out at any time. See our Privacy Policy.